UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/035,817	10/25/2001	Edward Scheidt	STSPT34	1778

49691 7590 04/07/2006

IP STRATEGIES
12 1/2 WALL STREET
SUITE I
ASHEVILLE, NC 28801

EXAMINER	
ZIA, SYED	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 04/07/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/035,817	SCHEIDT ET AL.	
	Examiner	Art Unit	
	Syed Zia	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 January 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-38* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-38* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

This office action is in response to amendment filed on January 17, 2006. Original application contained Claims 1-38. Applicant previously amended Claim 1.No amendment was filed this time. Therefore, presently claims 1-38 are pending.

Response to Arguments

1. Applicant's arguments with respect to claims 1-38 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

1. Claims 1-38 are rejected under 35 U.S.C. 103(a) as being unpatentable over by Glass (U. S. Patent 6,553,494), and further in view of Sudia (U. S. Patent 5,659,617).

2. Regarding Claim 1, Glass teaches and describes an electronic signature device comprising a processor, a memory, a user input device including a first signature input device, and a device interface, all commemoratively connected by at least one bus, a method of personalizing the electronic signature device to a user (Fig.1-5), comprising:

receiving a digitized written user signature of the user via the first signature input device, generating a user public key based on said signing private key and said prime and base parameters; generating a biometric electronic template based on said digitized written user signature; and storing said prime, sub-prime, and base parameters, said signing private and public keys, and said biometric electronic template in the memory (col.7 line 36 to col.9 line 52).

Although the system disclosed by Glass shows all the features of the claimed limitation, but Glass does not specifically disclose generating a prime parameter, a sub-prime parameter, and a base parameter; generating a signing private key; generating a signing public key based on said prime, sub-prime, and base parameters.

In an analogous art, Sudia, on the other hand discloses computing environment that relates to methods and apparatus for securely using digital signature in a cryptographic system by generating a prime parameter, a sub-prime parameter, and a base parameter; generating a signing private key; generating a signing public key based on said prime, sub-prime, and base parameters (i.e. multiple attributes)(col.13 line 18 to line 33).

Therefore, It would have been obvious to one ordinary skilled in the art at the time of invention to combine the teachings of Glass and Sudia, because Sudia's method of encrypting/decrypting of monitored data by using published primary keys with multiple attributes would not only promote security structure in the system of Glass during receiving digitized data from host input

computing devices but will also provide safeguards against attempt by unauthorized person to breach security of system.

3. Regarding Claim 26, Glass teaches and describes an electronic signature device comprising a processor, a memory having a biometric electronic template, a prime parameter, a sub-prime parameter, and a base parameter, user public data comprising a user public key, and a user private key stored therein, a user interface comprising a signature input device, a device interface adapted to interface a computer, and at least one bus operably connected to the processor, the memory, the user interface, and the device interface, a method of originating an electronically signed transaction (Fig.1-5), said method comprising:
verifying whether a user is permitted to originate the electronically signed transaction with the electronic signature device, comprising: receiving a digitized written originator signature via the user interface, and comparing said digitized mitten originator signature against the biometric electronic template to produce a first verification result; receiving a transaction package through one of the user interface and the device interface; combining said transaction package and one of said digitized originator signature and a digitized user signature extracted from the biometric electronic template to produce an originator signature block; generating an ephemeral private key based on the prime, sub-prime, and base parameters;, the user public key, and the prime parameter; encrypting said originator signature block with said shared encryption key to produce an encrypted signature block; combining said encrypted signature block, said ephemeral private key, the prime parameter, and at least a portion of the user public data to produce an

electronically signed transaction; and if the user is verified, providing said electronically signed transaction via the device interface (col.7 line 36 to col.9 line 52).

Although the system disclosed by Glass shows all the features of the claimed limitation, but Glass does not specifically disclose generating an ephemeral public key based on said ephemeral private key and the prime and base parameters; generating a shared encryption key based on said ephemeral public key.

In an analogous art, Sudia, on the other hand discloses computing environment that relates to methods and apparatus for securely using digital signature in a cryptographic system by generating a prime parameter, a sub-prime parameter, and a base parameter; generating a signing private key; generating a signing public key based on said prime, sub-prime, and base parameters (i.e. multiple attributes)(col.13 line 18 to line 33).

Therefore, It would have been obvious to one ordinary skilled in the art at the time of invention to combine the teachings of Glass and Sudia, because Sudia's method of encrypting/decrypting of monitored data by using published primary keys with multiple attributes would not only promote security structure in the system of Glass during receiving digitized data from host input computing devices but will also provide safeguards against attempt by unauthorized person to breach security of system.

4. Claims 2-25, and 27-37 are rejected applied as above rejecting claims 1, and 26. Furthermore, the system of Glass and Sudia teaches and describes, wherein:

As per claims 2-4, and 27, said prime, sub-prime, and base parameters are based on Diffie-Hellman parameters, and said prime, sub-prime, and base parameters are generated based on a seed value, and the seed value is one of a random value and a pseudorandom number (Glass:col.1 line 60 to col.2 line 20, and Sudia: col.13line 18 to line 33).

As per Claim 5, the seed value is received from the user via the user interface (col.2 line 21 to line 30).

As per Claim 6 the user interface further comprises a password input device, and said method further comprises: receiving a user password via the password input device; generating a password encryption key based on the user password; encrypting a known value with the password encryption key to produce an encrypted output; and storing the encrypted known value in the memory (Glass:col.4 line 26 to line 56).

As per Claim 7, and 29, said known value is said biometrics electronic template (Glass:col.4 col.5 line 12 to line 30, and col.9 line 10 to line 15).

As per Claims 8-17, and 30-31, receiving said digitized user signature is repeated at least once. receiving said digitized user signature and generating said biometrics electronic template are repeated at least once, said biometric electronic template is generated based on a mathematic transformation of said digitized written user signature, the mathematical transformation is a Fourier transformation, the electronic signature device is communicatively connected to a certificate authority via the device interface, and said method further comprises: sending a certificate request to the certificate authority; receiving a certificate package from the certificate authority, and storing said certificate package in the memory, said certificate request comprises said user public key, said certificate request further comprises at least one of said prime, sub-

prime, and base parameters, said certificate request comprises said user public key and said prime parameter, said certificate package comprises a digital certificate, and said certificate package comprises a digital certificate and a root value (Glass: col.4 col.3 line 29 to line 67).

As per Claims 18-23, the device interface is a card interface, the electronic signature device further comprises a power source that is at least one of a battery and the computer interface, the first signature input device is integral with the electronic signature device, the first signature input device is connected to the at least one bus through the device interface, and at least a portion of said user interface is integral with the electronic signature device, and at least a portion of said user interface is connected to the at least one bus through the device interface (Glass: Fig.3-5, and col.6 line 47 to col.7 line 12).

As per claims 24-25, said user public key is one of a random number and a pseudorandom number, and said user public key is smaller than said sub-prime parameter (Glass: col.3 line 51 to line 64, and Sudia: col. 13line 18 to line 33)).

As per Claim 28, the user interface further comprises a password input device, the memory has further stored therein an encrypted known value, and verifying whether the user is permitted to originate the electronically signed transaction with the electronic signature device further comprises receiving a user password via the password input device; generating a password encryption key based on the user password; decrypting the encrypted known value with said password encryption key to produce a second verification result (Glass: col.4 line 26 to line 56).

As per Claim 32, comparing said digitized written originator signature against the biometric electronic template comprises: generating a temporary template based on said digitized

written originator signature, and comparing said temporary template to the biometric electronic template (Glass: col.6 line 28 to line 60, and col.9 line 16 to line 36).

As per Claim 35, said digitized mitten originator signature against the biometric electronic template comprises: generating a temporary signature based on the biometric electronic template, and comparing said temporary signature to said digitized written originator signature (Glass: col.6 line 28 to line 60, and col.9 line 16 to line 36).

As per Claim 33-34, and 36-38, said temporary template is generated based on a mathematic transformation of said digitized written originator signature, the mathematical transformation is a Fourier transformation, and the at least a portion of the user public data comprises the user public key (Glass: col.3 line 29 to line 67).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Syed Zia whose telephone number is 571-272-3798. The examiner can normally be reached on 9:00 to 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

sz
March 23, 2006